IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF BLACK APPLE IPHONE IN BLACK CASE WITH SIM CARD TAPED TO THE BACK	**Crim. No. 21-mj-336** **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Adam Sucheski, a Special Agent with the Federal Bureau of Investigation, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is being made in support of an application for a search warrant for a black Apple iPhone in a black case, with a SIM card taped to the back, further described in Attachment A (hereinafter the "SUBJECT DEVICE"), to search for evidence, contraband, fruits and instrumentalities, further described in Attachment B, of violations of 18 U.S.C. § 2113(d) (armed bank robbery) and 18 U.S.C. §924(c) (using, carrying or brandishing a firearm during or in furtherance of a crime of violence).
2. I have been a Special Agent of the FBI for over 14 years, and am currently assigned to the Philadelphia Division, Fort Washington Resident Agency where I have investigated federal criminal violations related to armed robberies, fugitives, art theft, drug trafficking, bank robberies, counterintelligence, computer intrusions, fugitives, child exploitation, sextortion and threatening communications among other crimes**.**
3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant, and it does not set forth all of my knowledge about this matter.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Eastern District of Pennsylvania is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

LEGAL AUTHORITY

5. 18 U.S.C. § 2113(a) states that "Whoever, by force and violence, or by intimidation, takes, or attempts to take, from the person or presence of another, or obtains or attempts to obtain by extortion any property or money or any other thing of value belonging to, or in the care, custody, control, management, or possession of, any bank, credit union, or any savings and loan association" shall be guilty of an offense.

6. 18 U.S.C. 2113(d) makes it a crime to commit the offense of bank robbery by assaulting or putting in jeopardy the life of any person by the use of a dangerous weapon or device.

7. 18 U.S.C. § 924(c) makes it a crime, during and in relation to any crime of violence to use and carry a firearm, or in furtherance of any such crime, to possesses a firearm, or brandish a firearm.

PROBABLE CAUSE

8. On October 19, 2020, at approximately 8:30 a.m., Perkasie Borough Police Department was dispatched to a silent holdup alarm at the Quakertown National Bank (QNB) located at 607 West Chestnut Street, Perkasie Borough, Bucks County, Pennsylvania, which is in the Eastern District of Pennsylvania.

9. The tellers reported to police that a white male, approximately 5'6" to 5'7" tall, entered the bank following a teller who had arrived to open the bank. The suspect was wearing a dark ski mask with a hood covering his head and all dark clothing. The suspect was also wearing black boots and had a dark colored backpack. The suspect announced a robbery and demanded that the safe be opened. The suspect was told that another employee was needed to open the vault. Another employee entered the bank and the suspect took all the phones from the three employees present and had them open the safe. The suspect was then given two cash drawers from the safe containing U.S. currency. The suspect then demanded the cash from the tellers' drawers. The cash from two teller drawers was provided. The suspect at one point produced a small handgun from his pocket and stated that he did not want to hurt anyone. Prior to leaving, the suspect attempted to close the vault door locking the employees inside, however he could not secure the door.

10. I received notification of the activation of electronic tracking devices secreted in the money given to the subject. I observed that the tracking devices were active and were traveling south from the bank toward Conshohocken, Pennsylvania.

11. The tracking devices stopped in the area of 400 River Road, Conshohocken, Montgomery County, Pennsylvania, also located in the Eastern District of Pennsylvania.

12. Pennsylvania State Police Trooper Thomas Yates responded to the area to investigate and located a white work trailer (the "work trailer") at the Republic Services River Road Transfer Station. Trooper Yates entered the work trailer and observed CHRISTOPHER LARUE standing at an open locker with the name "LARUE" displayed on it. Trooper Yates advised that he observed a black backpack in the open locker, which was consistent

with the item described by the tellers. Additionally, LARUE was visibly upset and agitated upon seeing Trooper Yates.

13. Trooper Yates attempted to secure LARUE for an investigatory detention and grabbed LARUE's left hand to apply handcuffs. LARUE began to struggle with the Trooper and attempted to stop his attempts to detain him. LARUE then drew a small silver handgun, later determined to be a North American Arms Guardian .32 caliber pistol, with his right hand and pointed it over his left shoulder at Trooper Yates's head and stated "Do you want to fucking die today?" while pulling the trigger multiple times. The firearm did not discharge a round.

14. To secure LARUE, Trooper Yates released his grip on LARUE's hand, at which time LARUE racked the slide on the firearm to load the weapon. Trooper Yates was able to take physical control of LARUE and successfully secured him in handcuffs.

15. The investigating police departments, Perkasie Borough and the Pennsylvania State Police, obtained search warrants for the work trailer and LARUE's vehicle. The search of the work trailer, including LARUE's locker, resulted in the recovery of electronic tracking devices consistent with those utilized by QNB Bank, U.S. currency, a box of .32 caliber ammunition, a knit hat with eye holes, a magazine for a .32 caliber firearm, black sweatpants, a black Apple iPhone in a black case (the SUBJECT DEVICE), and other items.

16. Also recovered from the backpack inside the locker were "bait bills" which had been reported stolen from the bank. "Bait bills" are a pre-selected and recorded set of U.S. currency of which the bank maintains a record of the serial numbers. I have confirmed

that the serial numbers of the money stolen from QNB Bank in Perkasie on October 19, 2020 matched the recovered "bait bills" inside the backpack from LARUE's locker.

17. On October 20, 2020, a representative of the Federal Deposit Insurance Corporation (FDIC) confirmed that the QNB Bank branch noted above was insured at the time of the bank robbery.

18. On December 15, 2020, your Affiant took custody of the evidence items seized from the work trailer from the Pennsylvania State Police, including the SUBJECT DEVICE. The SIM card had been removed by the investigators and was taped to the back of the SUBJECT DEVICE. The SUBJECT DEVICE has been in the custody of FBI Philadelphia since then.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER/PHONE SYSTEMS

19. Your Affiant is aware that in today's age of technology with the ease of access to information, people utilize their cellular telephones to conduct various activities to include searching the Internet for information, seeking maps and directions for locations, reviewing the operating hours of businesses and conducting searches about committing or hiding crimes. Your Affiant is aware that bank robbers often research possible locations for robberies. This research has included location, hours of operation, security features, routes to and from the bank, and police response and bank security techniques. In addition, people who utilize firearms to commit crimes often use their cell phones to research different types of firearms and ammunition and how and where to obtain firearms and ammunition.

20. Searches and seizures of evidence from computer devices, cell phones, smart phones, and GPS's commonly require agents to download or copy information from the

devices and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, cell phones, smart phones, GPS's, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer and electronic systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

SEARCH METHODOLOGY TO BE EMPLOYED

21. To search for electronic data contained in computer, phone, or electronic device hardware, computer, phone, or electronic device software, and/or memory storage devices, the examiners will make every effort to use computer forensic software to have a computer search the digital storage media. This may include the following techniques (the following is a nonexclusive list, as other search procedures may be used):

a. searching for image and video files ;

b. surveying various file directories and the individual files they contain;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

e. scanning storage areas;

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B;

g. searching for malware in order to evaluate defenses, such as viruses; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

ABILITY TO RETRIEVE DELETED FILES

22. Computer files or remnants of such files on traditional or conventional mechanical computer hard drives can typically be recovered months or even years after they have been downloaded onto the hard drive, deleted or viewed via the Internet. Electronic files downloaded to the hard drive or storage device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from these conventional types of hard drives depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits.

23. Other than the conventional mechanical hard drives that are traditionally in computers, becoming more prevalent are flash memory based hard drives and devices. This technology has been traditionally used for small thumb drives where files and data are stored electronically, but has since evolved and is being used in computer hard drives known as "solid state hard drives" or SSD's and also being used in cell phones and smart phones. These devices do not operate like mechanical hard drives when it comes to how files and data are stored and deleted. These devices can move data around on the drive to maximize storage space and longevity of the drive, compress data, and may use different deletion techniques for how a deleted file is handled and overwritten. Because of how these flash, memory-based drives function it may limit how much data, if any, can be recovered from these types of devices.

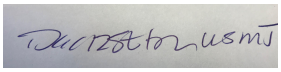
CONCLUSION

24. Based upon the information above I respectfully submit that there is probable cause to believe that evidence, contraband, fruits and instrumentalities further described in Attachment B, of violations of 18 U.S.C. § 2113(d) (armed bank robbery) and 18 U.S.C. § 924(c) (using, carrying or brandishing a firearm in furtherance of a crime of violence) will be located in the SUBJECT DEVICE, further described in Attachment A, and request that a search warrant be issued.

Respectfully submitted,

/s/ Adam Sucheski
Adam Sucheski, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to
before me this 23rd day of February, 2021.


David R. Strawbridge, USMJ
2021.02.24 10:19:10 -05'00'

HONORABLE DAVID R. STRAWBRIDGE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

A black Apple iPhone in a black case with SIM card taped to the back, currently in the FBI Fort Washington Resident Agency evidence storage, 501 West Office Center Drive, Suite 200, Fort Washington, PA, 19034.

ATTACHMENT B

Particular Things to be Seized

Evidence of violations of 18 U.S.C. §§ 2113(a) and 924(c) including the following:

1. Visual depictions of firearms, banks, security systems, alarms, surveillance images, maps, on whatever medium (e.g. digital media, optical media, books, magazines, photographs, negatives, videotapes, CDs, DVDs, etc.), including those in opened or unopened e-mails. These include both originals and copies, and authorization is granted to remove videotapes without viewing them at the time and place of seizure, and to view them at a later time.

2. All documents, to include in electronic form, and stored communications including contact information, text messages, call logs, voicemails, Internet searches, photographs, videos, and any other electronic data or other memory features contained in the devices and SIM cards including correspondence, records, opened or unopened e-mails, text messages, chat logs, and Internet history, pertaining to the possession, receipt, and access to firearms, and bank robbery planning to include searches for banks, police, security, alarms and other similar terms.

4. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, as well as all records relating to the ownership or use of the computer equipment or electronic devices.

5. All records which evidence operation or ownership or use of the device, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on the device.

6. All computer or electronic device passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.

7. Evidence and contents of logs and files on a computer, electronic device, or storage device, such as those generated by the computer's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the computer or device at the time any of the items described in paragraph 1-3 were created, sent, received, or viewed. Also, any malware resident on the computer/phone or device.